

United States Court of Appeals
FOR THE EIGHTH CIRCUIT

No. 03-3615

United States of America,

Appellee,

v.

Wesley George Thorn,

Appellant.

*
*
*
*
*
*
*
*
*

Appeal from the United States
District Court for the
Western District of Missouri.

Submitted: February 10, 2004

Filed: July 13, 2004

Before LOKEN, Chief Judge, BOWMAN and WOLLMAN, Circuit Judges.

BOWMAN, Circuit Judge.

Defendant Wesley Thorn was charged with one count of possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B) and 2252(b) (2000). The District Court¹ denied Thorn's motion to suppress evidence obtained in a search of his office at the Missouri Division of Child Support Enforcement ("DCSE"), and he

¹The Honorable Ortrie D. Smith, United States District Judge for the Western District of Missouri, adopting the report and recommendations of the Honorable James C. England, United States Magistrate Judge for the Western District of Missouri.

entered a conditional plea of guilty to the charge.² He was sentenced to twenty-seven months of imprisonment with three years of supervised release. Thorn appeals the District Court's denial of his motion to suppress.

The child pornography at issue was discovered on computer media found in Thorn's DCSE office in Joplin, Missouri, which had been searched during an investigation of claims of workplace misconduct on Thorn's part. On February 8, 2002, Valerie Davis, Thorn's supervisor in the Joplin office, began investigating purported workplace misconduct after she received complaints that Thorn was inaccessible and had copied and distributed non-work-related e-mail messages throughout the office. To determine whether Thorn had used his DCSE computer to distribute the offending e-mail, Davis instructed a computer information technician to conduct a remote examination of the contents of the hard drive of the computer. The technician found a copy of the e-mail on the hard drive and further discovered that Thorn had used his computer to access adult pornographic websites. After learning that Thorn had used his computer to access pornographic materials in contravention of express policy, Davis contacted Dan Padfield, Regional Manager of DCSE in charge of the Joplin office. Thorn's supervisors decided to place him on administrative leave pending further investigation of his computer misconduct.

On February 11, 2002, Padfield visited the Joplin office in order to secure Thorn's computer for further investigation. He ultimately took the computer tower and numerous floppy disks from Thorn's office, in order to examine their contents to determine the scope of Thorn's violations of the agency's computer-use policy. Thorn called in sick and was informed of the decision to place him on leave. He requested permission to access his office in order to retrieve certain tax documents. Padfield

²A conditional guilty plea reserves to the defendant the right to appeal, after the trial court has accepted the plea and imposed judgment, the denial of the defendant's motion to suppress evidence that, in the defendant's view, was illegally obtained.

informed Thorn that he could not remove anything from his office, but offered to retrieve the tax forms for him. Thorn agreed to this arrangement and gave instructions as to where the documents were located in the desk. In his search for these materials, Padfield discovered pornographic material interspersed with other documents in the desk. Padfield then informed Dianne Goetz, human resources manager of DCSE, of the discovery of further pornographic materials. Goetz decided to terminate Thorn's employment for his violations of the agency's code of conduct, its sexual-harassment policy and its computer-use policy. Padfield and Davis then contacted investigators at the Division of Legal Services ("DLS") and requested they visit the Joplin office and inventory the contents of Thorn's office and computer media for the purpose of setting forth the reasons for the termination of his employment. In examining the contents of the floppy disks Padfield had taken from Thorn's office, a DLS investigator discovered images of child pornography. Because he had discovered possibly criminal contraband, he immediately stopped cataloguing the contents of the disks and instructed another DLS investigator to contact law-enforcement officers at the Joplin Police Department.

DCSE is an agency within the Missouri Department of Social Services ("DSS"). DSS has a communication policy which explicitly forbids personal use of the agency's computer systems and limits access to certain materials: "Electronic mail is to be used for work-related reasons only. All electronic messages, documents . . . or pictures that are . . . sexual, pornographic, inappropriate, harassing . . . are prohibited." Dept. of Soc. Servs. Memo on Communication Sys. (Jan. 3, 2000). Furthermore, this policy imposes an affirmative duty upon agency employees to report any suspected abuse of the agency's computer systems: "Employees should immediately report to their supervisors the receipt of any inappropriate and unsolicited electronic communications, any accidental access to Internet sites, and any unauthorized use of DSS information technology and systems by other employees" *Id.* In addition, the policy expressly provides that "Employees do not have any personal privacy rights regarding their use of DSS information systems and

technology. An employee's use of DSS information systems and technology indicates that the employee understands and consents to DSS'[s] right to inspect and audit all such use as described in this policy." Id. (emphasis in original). Thorn acknowledged this policy in writing when he requested computer access in 2000. Online Security Access Request (Nov. 3, 2000).

After getting affidavits from the DCSE and DLS officials, who set forth their discovery of adult and child pornographic materials, Lieutenant Carl Francis of the Joplin Police Department obtained a search warrant on February 15, 2002, to permit him to search for and seize such evidence from Thorn's office. One month later, Francis obtained another warrant to permit the examination of the contents of the seized computer media. The searches pursuant to these warrants uncovered child pornography in the desk and filing cabinet of Thorn's office and on certain floppy disks removed from the office. Thorn, having been charged with the offense to which he later entered a conditional plea of guilty, moved to suppress all evidence from the warrantless search of his office conducted by Padfield and the DLS investigators. In addition, he sought to suppress all evidence obtained under the two search warrants. The District court denied this motion, Thorn entered his plea, and the District Court entered judgment convicting Thorn as charged. This appeal followed. We review a denial of a motion to suppress *de novo*, but review any underlying factual determinations for clear error. United States v. Velazquez-Rivera, 366 F.3d 661, 664 (8th Cir. 2004).

A plurality of the Supreme Court has held that public employers may, consistent with the Fourth Amendment, conduct workplace searches without a warrant and without probable cause when there are reasonable grounds to suspect work-related misconduct. O'Connor v. Ortega, 480 U.S. 709, 725–26 (1987) (plurality opinion); see also O'Connor, 480 U.S. at 732 (Scalia, J., concurring in judgment and concluding government searches to investigate work-related misconduct "do not violate the Fourth Amendment"). A workplace search by a

government employer implicates an employee's Fourth Amendment rights only if the employer's conduct infringes upon the employee's reasonable expectations of privacy. O'Connor, 480 U.S. at 715; *see also* United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002) ("[I]n order to find a violation of the Fourth Amendment, there must be a legitimate expectation of privacy in the area searched and the items seized."), cert. denied, 538 U.S. 993 (2003). Thorn did not have any legitimate expectation of privacy with respect to the use and contents of his DCSE computer. He was fully aware of the computer-use policy, as evidenced by his written acknowledgment of the limits imposed on his computer-access rights in 2000. The policy specifically bars certain unauthorized use of DSS computers and further provides that employees have no personal right of privacy with respect to their use of the agency's computers. Furthermore, the policy explicitly provides DSS the right to access all of the agency's computers in order to audit their use. In light of the express limits placed upon his computer use by the agency's computer-use policy, the District Court correctly determined that Thorn had no legitimate expectation of privacy in the contents of his office computer. *See* United States v. Angevine, 281 F.3d 1130, 1134–35 (10th Cir.) (rejecting claim of reasonable expectation of privacy in data an employee downloaded from the Internet to a state university's computers when the university had an express policy that reserved the right to randomly audit Internet use), cert. denied, 537 U.S. 845 (2002); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (concluding that government employee had no legitimate expectation of privacy in files downloaded from the Internet when government employer had express policy limiting computer usage to official government business and permitted random audits of computer usage to ensure proper use of government resources); *cf.* United States v. Slanina, 283 F.3d 670, 676–77 (5th Cir.) (upholding search but determining that employee had legitimate expectation of privacy in contents of office computer when government employer had not disseminated any policy limiting personal use of the computer and employee's computer was password-protected), vacated on other grounds by 537 U.S. 802 (2002), on appeal after remand 359 F.3d 356, 358 (5th Cir. 2004) (per curiam) (reaffirming validity of workplace search); Leventhal v. Knapek,

266 F.3d 64, 73–74 (2d Cir. 2001) (determining that an employee had a legitimate expectation of privacy in the contents of his office computer but noting the absence of a policy explicitly limiting the scope of privacy in the computer).

Although any expectation of privacy in the contents of his office computer was not reasonable, Thorn may have had a legitimate expectation of privacy in his DCSE office, desk, and filing cabinet. Nonetheless, any such expectation was limited in scope because other DCSE employees had keys that allowed them to access the office and the contents of the desk and cabinets. Furthermore, the office, desk, and filing cabinet were all state-issued property and not Thorn's personal belongings. See O'Connor, 480 U.S. at 716 (plurality opinion) (recognizing offices, desks and filing cabinets as part of the workplace that employers may search for evidence of work-related misconduct); cf. Gossmeier v. McDonald, 128 F.3d 481, 490 (7th Cir. 1997) (refusing to find a legitimate expectation of privacy in the contents of filing cabinets kept in a government office despite the fact that they were *not* state property and, in fact, were purchased by the office occupant's own funds).

Assuming arguendo that Thorn had some minimal expectation of privacy in his office, desk and filing cabinet, the searches of these items by Padfield and the DLS investigators did not violate the Fourth Amendment's prohibition against unreasonable searches. Under O'Connor, a public employer can investigate work-related misconduct so long as any search is justified at inception and is reasonably related in scope to the circumstances that justified it in the first place. 480 U.S. at 726. A search is justified at inception "when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct." Id. The scope of a search is reasonable when the measures adopted are reasonably related to the objectives of the search and are not unnecessarily intrusive. Id.

Because Thorn had no legitimate expectation of privacy with respect to his use of his office computer, the initial remote search of this computer did not violate the Fourth Amendment. DCSE officials initially entered Thorn's office merely to secure his computer tower for a more thorough examination of its contents; they did not search other areas of the office until Thorn instructed Padfield to retrieve the tax forms from his desk. In directing Padfield to secure these documents, Thorn consented to Padfield's initial search of the desk. While searching for the forms, Padfield discovered computer-generated pornographic stories and pictures throughout the desk; this discovery allowed DCSE to expand the scope of the investigation to include places and items where computer-generated pornographic materials could be stored, such as on floppy disks. See, e.g., Leventhal, 266 F.3d at 76–77 (recognizing that evidence of misconduct uncovered by an initial workplace search may provide justification for an expanded investigation of the misconduct). Padfield was thus justified in seizing Thorn's floppy disks from the desk in order to determine if they contained pornography. See Slanina, 283 F.3d at 679–80 (concluding that government employer was justified under O'Connor in conducting a full search of computer hard drive and zip disks for further evidence of misconduct once employer had determined employee had accessed pornographic materials with the computer). The further examination of the contents of the office and the floppy disks by DLS investigators was reasonable in light of DCSE's decision to terminate Thorn because the investigators were merely cataloguing evidence of Thorn's work-related misconduct in order to document the reasons for the termination in the event of legal action by Thorn. Immediately upon discovering evidence of possible child pornography, the investigators halted their inventory and notified local law-enforcement officials.

At no time did the agency's investigation into Thorn's work-related misconduct devolve into a de facto criminal investigation that should have been conducted pursuant to a warrant. As evidence of widespread misconduct surfaced, through the audit of Thorn's computer use and through the accidental discovery of pornographic

materials during the retrieval of Thorn's tax forms, DCSE had every right to investigate the scope of this misconduct. After the computer-use audit and consent search of the desk, the permissible scope of the search for evidence of Thorn's work-related misconduct reasonably included Thorn's office, desk, and filing cabinet. The various warrantless searches conducted by DCSE and DLS officials did not violate the Fourth Amendment. The District Court therefore properly refused to suppress evidence discovered during these searches. This evidence provided sufficient probable cause for the February search warrant, which permitted the search for and seizure of contraband, photographs, printed materials and electronic storage media by the Joplin Police Department. The District Court properly refused to suppress evidence discovered in the execution of this warrant as well.

The March 15 search warrant was a supplemental warrant that Lieutenant Francis sought before examining the contents of computer media seized during the execution of the February warrant. The government conceded to the Magistrate Judge that this warrant was fatally deficient on its face because it failed to set forth the factual basis for probable cause to believe that child pornography would be discovered in the computer media at issue. Nonetheless, evidence discovered from the police search of the floppy disks need not be suppressed because the March warrant was surplusage and was not required to permit law enforcement officials to examine the contents of the seized computer media. The February warrant, which explicitly authorized the search and seizure of electronic storage media containing images of minors involved in sexual acts, was sufficient to provide the authority to examine the contents of the various computer-related media. See, e.g., United States v. Upham, 168 F.3d 532, 536 (1st Cir.) ("The warrant explicitly authorized the seizure of both the computer plus diskettes and the unlawful images. The images . . . were 'inside' the computer or diskettes. The extraction of unlawful images from within the computer and diskettes was therefore contemplated by the warrant."), cert. denied, 527 U.S. 1011 (1999); cf. United States v. Wright, 704 F.2d 420, 422 (8th Cir. 1983) (per curiam) (holding that warrant permitting search for drugs within a house

permitted the search of a safe within the house that might reasonably have contained drugs). The District Court properly refused to suppress evidence from the examination of the contents of the various floppy disks taken from Thorn's office.

The District Court's decision to deny Thorn's motion to suppress, leading to the acceptance of his conditional plea of guilty and the imposition of the resulting conviction, is affirmed.
